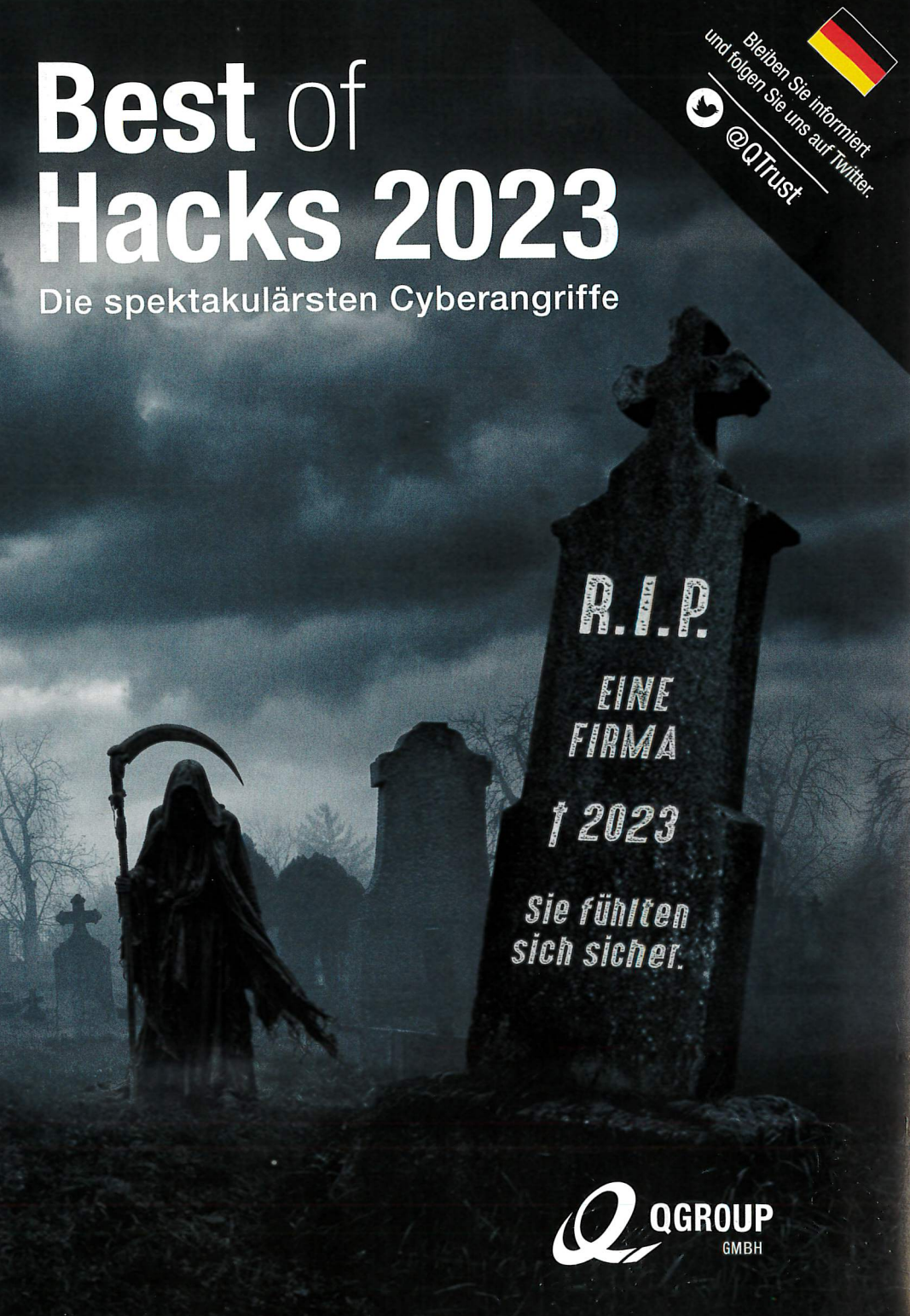
Best of Hacks 2023

Die spektakulärsten Cyberangriffe



QGROUP
GMBH

VORWORT zur Gesamtausgabe 2023

Auch das Jahr 2023 war geprägt von vielen bedeutenden und dramatischen Ereignissen und Entwicklungen. Der anhaltende Krieg in der Ukraine gibt auch im dritten Jahr Anlass zu großer Sorge. Weitere geopolitische Spannungen entstanden, darunter der Krieg zwischen der Hamas und Israel, der erneut das ohnehin fragile Gleichgewicht im Nahen Osten erschütterte und zu internationalen Spannungen führte, sowie die Drohgebärden Chinas gegenüber Taiwan, die bislang jedoch glücklicherweise noch nicht in Kampfhandlungen mündeten.
Die Progression der Klimakrise und ihre immer häufiger auftretenden Auswirkungen führten zu intensiveren Diskussionen und Forderungen nach umfassenden Maßnahmen zum Schutz unserer Umwelt. Gleichzeitig erlebten wir bedeutende technologische Fortschritte, jedoch auch neue Herausforderungen im Bereich des Datenschutzes und der Cybersicherheit, insbesondere im Zusammenhang mit künstlicher Intelligenz.

Auch 2023 gab es wieder »leisere«, aber nicht weniger disruptive Ereignisse, die unsere Gesellschaft stark und nachhaltig beeinflussten: Zahlreiche Unternehmen wurden gehackt, getäuscht, bedroht, erpresst und ihre IT-Systeme mit Schadsoftware infiziert. Laut einer Studie von Cybersecurity Ventures fand 2023 alle 39 Sekunden ein Cyberangriff statt. Im Jahr 2022 lag dieser Wert noch bei 44 Sekunden. Für das vergangene Jahr stechen vor allem drei Begrifflichkeiten hervor, die IT Security-Verantwortliche herausfordern: Malware, Ransomware und Phishing. Diese Angriffspfade sind umso problematischer, da die Bedrohungsakteure dazu übergegangen sind, soziale Techniken und künstliche Intelligenz in ihre Angriffsmethoden zu integrieren.

Ein besonderer Fokus lag auf Datenschutzverletzungen im Zusammenhang mit Ransomware-Angriffen. Im Jahr 2023 wurden mehr als 45 Millionen Datensätze offengelegt. Das entsprach zwar in etwa dem Niveau des Vorjahres, führte aber erneut zu erheblichen finanziellen Schäden und Rufschädigungen. Beispiele wie Angriffe auf die Unternehmen Uber, Twitter, Samsung und diverse Krankenkassen veranschaulichen die Auswirkungen solcher Angriffe.

Weitere Beispiele für erfolgreiche Cyberattacken sind Organisationen und Unternehmen wie die Hochschule Hannover, der Deutsche Bundestag, die Websites mehrerer deutscher Flughäfen, T-Mobile US, die US-Regierung und die NATO. Diese Angriffe verdeutlichen die ernsthafte Bedrohung durch Cyberkriminalität und die dringende Notwendigkeit, die digitale Sicherheit zu erhöhen.

Entstandene und möglicherweise noch entstehende Schäden lassen sich nicht genau beziffern oder vorhersagen. Kein Unternehmen, keine Behörde und keine Privatperson ist sicher und die Schäden können existenzbedrohend sein - nicht nur für einzelne Arbeitsplätze, sondern für gesamte Unternehmen. Es besteht dringender Handlungsbedarf, entsprechende Sicherheitsmaßnahmen zu ergreifen und die digitale Sicherheit zu erhöhen.

Die gute Nachricht ist, dass fast alle Fallbeispiele in dieser Broschüre hätten verhindert werden können - zum Beispiel durch den Einsatz sicherer Betriebssysteme, biometrischer Authentifizierung, durch die Absicherung administrativer Prozesse mit klarer Trennung von externen und internen Zugriffsrechten (Multi-Level Security) und dem frühzeitigen Aufbau eines IT-Immunsystems bestehend aus einer modernen EndPoint Protection-Lösung sowie qualifizierter Netzwerk-Forensik, Schwachstellenmanagement und Security Operations.

Todesanzeigen 1 ..... S. 4
Check4Hack ..... S. 18
Todesanzeigen 2 ..... S. 20
Strategiewechsel ..... S. 35

Gehen Sie mit uns neue Wege.
Wir kennen den Unterschied.

DEEZER

Was? Eine Attacke auf einen Deezer-Dienstleister ermöglichte den Raub von 230 Millionen Datensätzen.

Wie? Cyberangriff

Wann? Januar 2023

Schaden: Es wurden Daten von Vor- und Nachnamen, Geburtsdaten und E-Mail-Adressen von Nutzern erbeutet. Diese »nackten Daten« können angereichert werden und zu gut gemachten Phishing-Angriffen führen.

ROYAL MAIL

Was? Eine Cyberattacke legte den britischen Post-Dienstleister lahm.

Wie? Ransomware

Wann? Januar 2023

Schaden: Es kam zu einer schwerwiegenden mehrtägigen Unterbrechung der internationalen Export-Dienstleistungen.

SKY

Was? Unbekannte verschafften sich Zugang zu den Kundenkonten des Medienkonzerns.

Wie? Cyberangriff

Wann? Januar 2023

Schaden: Es konnten keine Anzeichen für einen konkreten Missbrauch dieser Daten nachgewiesen werden.

Doc Morris

Was? Die Online-Apotheke wurde gehacked und 20.000 Kundenkonten kompromittiert.

Wie? Cyberangriff

Wann? Januar 2023

Schaden: Unbekannten Täter änderten die Adressen von Kundenkonten und bestellten in deren Namen Medikamente.

Deutsche Flughäfen

Was? Die Webseiten mehrerer deutscher Flughäfen wurden attackiert und waren nicht erreichbar.

Wie? DDoS-Angriff

Wann? Februar 2023

Schaden: Zu möglichen Hintergründen gab es keine Angaben. Den Flughafenbetreibern zufolge gab es keine Auswirkungen auf den Flugbetrieb.

Dole

Was? Der weltgrößte Obst- und Gemüseproduzent wurde gehacked und erpresst. Daraufhin schaltete der Konzern seine Systeme in ganz Nordamerika ab.

Wie? Ransomware

Wann? Februar 2023

Schaden: Die Produktion in den USA wurde temporär eingestellt und viele Regale in den Läden blieben leer.
Die Höhe der Lösegeldforderung blieb unbekannt.

QTRUST® Check4Hack

Sind Sie sicher?

Finden Sie es heraus!

- Angriffsvektorenanalyse
- Netzwerkforensik
- Schwachstellenanalyse
- Passwortaudit
- Active Directory-Sicherheitsüberprüfung
- IoT-Analyse
- Penetrationstest
- Social Hack

QGROUP GMBH

WE SECURE IT.

FBI

Was? Die US-Bundespolizei war von einer Cyberattacke im internen Netzwerk betroffen.

Wie? Cyberangriff

Wann? Februar 2023

Schaden: Ein forensisches Analysenetzwerk des FBI wurde infiltriert. Nach Aussagen des FBI blieb der Schaden jedoch auf dieses Netzwerk beschränkt.

RUSSLAND

Was? Hacker haben in Russland Warnungen vor Luftangriffen über Radiosender, Sirenen und Textnachrichten verbreitet.

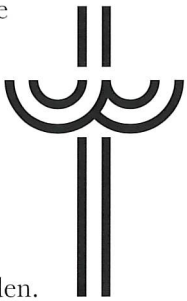
Wie? Cyberangriff

Wann? Februar 2023

Schaden: Die Bevölkerung war irritiert und wurde in Schrecken versetzt.

HOSPITAL CLINIC DE BARCELONA

Was? Ein Cyberangriff legte die Computer eines der größten Krankenhäuser in Barcelona in den Laboren, der Notaufnahme sowie der Apotheken lahm.



Wie? Ransomware

Wann? März 2023

Schaden: Hunderte Operationen und tausende Untersuchungen mussten abgesagt werden.

Ferrari

Was? Bei einem IT-Sicherheitsvorfall des Autoherstellers wurden Kundendaten erbeutet.
Dies führte zur Erpressung von Lösegeld.

Wie? Cyberangriff

Wann? März 2023

Schaden: Laut Ferrari wurden die betroffene Kunden informiert und es wurde kein Lösegeld gezahlt.
Der Geschäftsbetrieb war nicht eingeschränkt.

Stadtwerke

KARLSRUHE

Was? Hacker drangen in das Netzwerk der Stadtwerke Karlsruhe ein. Vermutlich hatten sie zuvor Daten eines hochrangigen Mitarbeiters erbeutet.

Wie? Cyberangriff

Wann? März 2023

Schaden: Die Stadtwerke informierten darüber, dass ihre versorgungsrelevante IT nicht betroffen gewesen sei und die Schadsoftware sich nicht ausbreiten konnte.

SMART / LAB

Was? Die Steuerung einer Ladesäule für E-Autos des bayrischen Anbieters für Elektromobilität war ungeschützt im Netz.

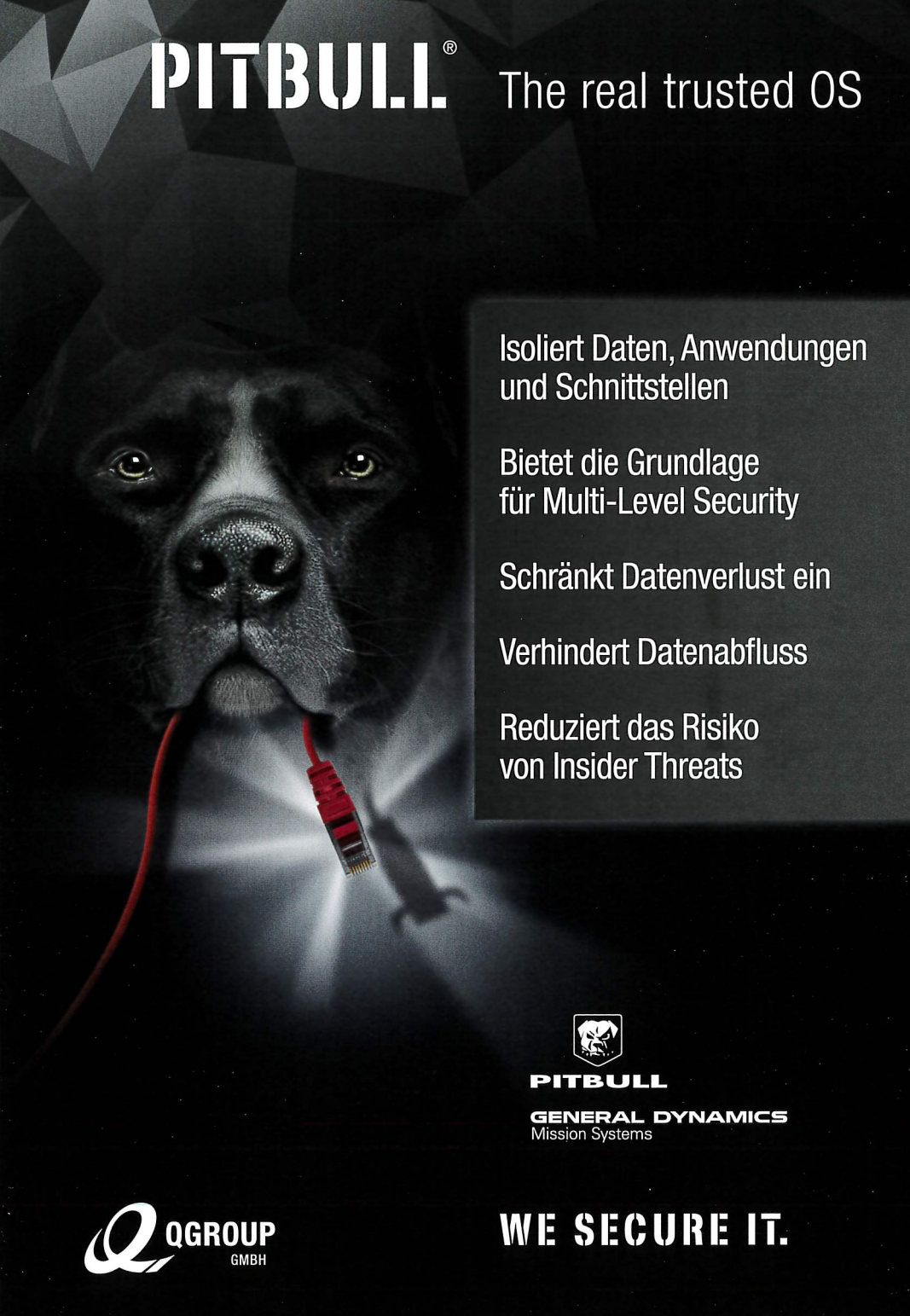
Wie? Datenverletzung

Wann? März 2023

Schaden: Angreifer konnten UIDs rauben, mit deren Hilfe sich Ladekarten klonen und auf Kosten ihrer Besitzer Autos laden lassen.
Die Schadenhöhe blieb unbekannt.

PITBULL®

The real trusted OS



Isoliert Daten, Anwendungen und Schnittstellen

Bietet die Grundlage für Multi-Level Security

Schränkt Datenverlust ein

Verhindert Datenabfluss

Reduziert das Risiko von Insider Threats

PITBULL

GENERAL DYNAMICS
Mission Systems

QGROUP GMBH

WE SECURE IT.

US-Regierung

Was? Durch ein Datenleck wurden Informationen zum Ukraine-Krieg offengelegt.

Wie? Datenverletzung

Wann? April 2023

Schaden: Es wurde eine unbefugte Weitergabe von sensiblem und geheimem Material festgestellt. Der Schaden ist nicht zu beziffern und die Folgen unabsehbar.

Rheinmetall
Automotive

Was? Der Rüstungskonzern wurde Opfer eines Cyberangriffs. Betroffen war das zivile Geschäft im Automotive-Sektor.

Wie? Cyberangriff

Wann? April 2023

Schaden: Die Schadenhöhe blieb unbekannt.

Nordrhein-Westfalen

Was? Eine Sicherheitslücke auf den Schulservern veröffentlichte tausende User-Daten.

Wie? Datenverletzung

Wann? April 2023

Schaden: Das gesamte Active Directory war zugänglich. Betroffen waren 16.000 Accounts mit Namen, E-Mails und Jobs.

adesso

Was? Der IT-Dienstleister wurde erfolgreich attackiert, verschwieg jedoch seinen Kunden – große Firmen und Bundesbehörden – die Kompromittierung.

Wie? Cyberangriff

Wann? April 2023

Schaden: Die Schadenhöhe blieb unbekannt. Die Unterlassung der Angriffsmeldung hatte jedoch dramatische Folgen.

T-Mobile USA

Was? Unbekannte erbeuteten auf den Systemen von T-Mobile zwar nur 836 jedoch um so wertvollere Datensätze mit Sozialversicherungsnummern.

Wie? Cyberangriff

Wann? Mai 2023

Schaden: Mit den gestohlenen Daten war es u. a. möglich, in fremdem Namen Kredite aufzunehmen, Bankkonten zu eröffnen oder Bestellungen zu tätigen.

Baseler Schulnetz

Was? 1,2 Terabyte an Daten von Baseler Schülern kursieren im Darknet. Diese stammen vom Baseler Bildungsserver.

Wie? Cyberangriff

Wann? Mai 2023

Schaden: Täter drangen in den Baseler Bildungsserver eduBS ein, luden dort Daten herunter und versuchten damit, den Kanton Basel-Stadt zu erpressen. Als dies scheiterte, wurden die Daten veröffentlicht.

Was? Nach einem Cyberangriff auf Deutschlands größte Werkstattkette waren verschiedene Dienste nicht oder nur »eingeschränkt erreichbar«.

Wie? Cyberangriff

Wann? Mai 2023

Schaden: Sowohl die Website als auch die telefonische Erreichbarkeit waren nach Angaben von ATU von der Attacke betroffen.

ABB

Was? Das Schweizer Technologieunternehmen wurde Opfer eines Ransomware-Angriffs.

Wie? Ransomware

Wann? Mai 2023

Schaden: ABB zahlte vermutlich das geforderte Lösegeld. Die Höhe des Erpressungsbetrages blieb unbekannt.

Handelsblatt

Was? Die Zeitung ist Kunde eines IT-Dienstleisters, der gehacked wurde und dessen IT komplett ausfiel.

Wie? Cyberangriff

Wann? Juni 2023

Schaden: Die Druckausgabe der Zeitung konnte vorübergehend nur in reduziertem Umfang herausgegeben werden.

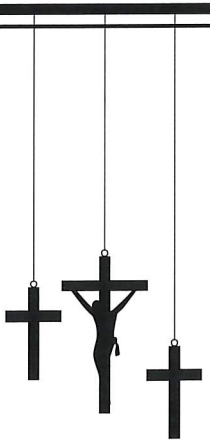
AfD

Was? Der Web-Auftritt der Partei war unzureichend gesichert.

Wie? Datenverletzung

Wann? Juni 2023

Schaden: Mitgliedsanträge waren über ein Web-Verzeichnis ohne weitere Schutzmaßnahmen direkt zugreifbar.



Incident? Notfall?

Kontaktieren Sie uns umgehend über unsere Hotline:

+49 69 17 53 63 - 047

In kritischen Momenten zählt jede Sekunde. Wenn Sie den Verdacht haben, dass Ihre IT-Systeme kompromittiert wurden, steht Ihnen die QGroup mit schneller und professioneller Hilfe zur Seite.

Unser Incident Response-Team ist rund um die Uhr erreichbar, um im Falle eines Cyberangriffs zu unterstützen.

Als vom BSI anerkannter APT Response-Dienstleister für Kritische Infrastrukturen verfügen wir über ein etabliertes Verfahren, das in enger Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik entwickelt wurde.

Dieses Verfahren ermöglicht es uns, schnell zu handeln, um den Schaden zu minimieren und eine weitere Ausbreitung der Bedrohung zu verhindern.

Wir sind für Sie da!

QGROUP GMBH

WE SECURE IT.

QTRUST CHECK4HACK®

Sind Sie sicher?

- **Ganzheitliche Übersicht zum Status Quo Ihrer IT-Sicherheit**
- **Optimale Grundlage für weitere Budgetplanung und Folgemaßnahmen**
- **Erkennen von unbekannten Gefahrenpotentialen und Eindringlingen**
- **Unterstützung bei der Umsetzung der Datenschutz-Grundverordnung (DSVGO)**

Reine Prävention ist unserer Erfahrung nach nicht mehr ausreichend. Zu häufig stellen wir fest, dass der Angriff, gegen den man sich schützen wollte, in der Vergangenheit bereits stattgefunden hat. Aber leider bemerken die wenigsten Unternehmen diese Angriffe. Aus diesem Grund haben wir ein ganzheitliches Security Assessment-Programm entwickelt – den Check4Hack. Hierbei kommen verschiedene Vorgehensweisen und Ansätze in Kombination mit hochspezialisierter Hard- und Software sowie Expertenwissen zur Anwendung. Im Gegensatz zu einem Penetrationstest prüfen wir hier nicht nur eine Auswahl möglicher Angriffsvektoren, sondern unsere Kunden erhalten ein umfassendes Bild zu aktuellen Kompromittierungen, den kritischsten Angriffsvektoren und deren Beseitigungsmöglichkeiten.

Angriffsvektorenanalyse Zusammen mit unseren Kunden erarbeiten wir den Status Quo der vorhandenen IT-Infrastruktur. Basierend auf unseren Erfahrungen im militärischen IT-Sicherheitsbereich identifizieren wir Angriffsvektoren, die wir in den anschließenden Tests ggf. zum Einsatz bringen.

Netzwerkforensik Dieses Modul erkennt Advanced Persistent Threats (APT), komplexe Malware, Exploits und Command & Control-Fernsteuerungen. Durch den Einsatz eines QTrust® U.F.N.T.A. (Universal Forensic Network Traffic Analyzer) können aktive Angreifer in Echtzeit erkannt und forensisch analysiert werden. So wird transparent, welche Daten ein Netzwerk infiltrieren oder welche gestohlen werden. Angriffe aus der Vergangenheit können aufgrund des Verhaltens kompromittierter Geräte ebenfalls nachgewiesen werden.

Schwachstellenanalyse Anhand der Ergebnisse der Angriffsvektorenanalyse werden u. a. unterschiedliche Vulnerability Scans auf die zu prüfenden Systeme gestartet. Ein Abschlussbericht bewertet die gefundenen Schwachstellen und Fehlkonfigurationen nach Kritikalität. Zusätzlich werden Möglichkeiten zur Beseitigung dieser Schwachstellen aufgezeigt. Hier liegt der Fokus darauf, in Zusammenarbeit mit unseren Kunden, die Relation zwischen den Untersuchungsergebnissen und den finanziellen und geschäftlichen Risiken herzustellen. So entsteht ein klares Bild, wie viel ein Angreifer investieren müsste, um die Informationssicherheit des Unternehmens zu kompromittieren.

Passwortaudit Passwörter eines Unternehmens werden mit Methoden wie Brute-Force, Wörterbuch-Attacke, bekannte Initialpasswörter sowie Kombinationen der genannten Methoden geprüft. Die daraus resultierenden Erkenntnisse geben darüber Aufschluss, welche Passwörter leicht zu kompromittieren sind. So können Maßnahmen zur Qualitätssteigerung der Passwörter eingeleitet werden.

Active Directory-Sicherheitsüberprüfung Das Active Directory (AD) kann durch Schwachstellen, wie etwa unsichere Prozesse, eingeführt durch Mitigationen oder veraltete Prozesse, zur Bedrohung für ein Unternehmen werden. Eine Kompromittierung des AD kann bis zum Vollzugriff auf alle Computer in der entsprechenden Domäne führen. Die AD-Sicherheitsüberprüfung deckt diese kritischen Lücken auf und unterstützt bei der Behebung der Schwachstellen.

Optionale Module

IoT-Analyse Eines der häufigsten Einfallstore für Hacker sind IoT-Geräte, wie z. B. Überwachungskameras, Access Points etc. Diese Geräte werden selten oder gar nicht gepatched und stehen aktuell oft nicht im Sicherheitsfokus. Die QGroup unterstützt Sie dabei, diese Lücke zu schließen.

Penetrationstest Ein Penetrationstest erfolgt in der Regel nach der Einführung eines neuen Systems, um dieses auf seine Angreifbarkeit zu prüfen oder nach einem Check4Hack, um die gefunden Schwachstellen manuell weiter zu verfolgen und zu untersuchen, wie weit man ins System vordringen könnte.

Social Hack Immer häufiger werden Methoden des Social Engineering genutzt, also soziale Angriffe auf Personen, um darüber die Chancen für einen erfolgreichen Angriff zu verbessern. Eine Überprüfung der technischen Abwehrfähigkeiten einer Organisation ist deshalb in vielen Fällen zu kurz gegriffen. Aus diesem Grund bieten wir mit dem QGroup Social Hack eine Sicherheitsüberprüfung an, die neben technischen Angriffsvektoren die Technik des Social Engineerings nutzt. Nach Durchführung eines Social Hack lassen sich ganzheitliche Verbesserungen für die Sicherheit der Organisation ableiten und entsprechendes Bewusstsein (Awareness) bei den Mitarbeitern schaffen.

ChatGPT

Was? Per Scraping öffentlicher Programmierprojekte soll ein Nutzer Zugang zu Hunderten API-Schlüsseln für GPT-4 erlangt haben.

Wie? Scraping

Wann? Juni 2023

Schaden: ChatGPT-Nutzer erhielten Zugang zu einem OpenAI-Konto mit einem Nutzungsbudget von 150.000 US-Dollar.

SPD

Was? Hackern ist es gelungen, auf E-Mail-Postfächer des SPD-Parteivorstands zuzugreifen.

Wie? Cyberangriff

Wann? Juni 2023

Schaden: Eine Sprecherin der SPD: »Es ist eine einstellige Anzahl von E-Mail-Konten von dem Angriff betroffen.«

DEUTSCHE BANK UND POSTBANK

Was? Bei einem Dienstleister der Deutschen Bank und der Postbank sind sensible Kundendaten abgeflossen.

Wie? Cyberangriff

Wann? Juli 2023

Schaden: Dadurch wurden unberechtigte Lastschriften ermöglicht. Die Schadenhöhe wurde nicht bekannt.

G✝✝gle Play Store

Was? IT-Sicherheitsforscher entdeckten Android-Malware im Google Play Store. Sie wurde 1,5 Millionen Mal installiert.

Wie? Cyberangriff

Wann? Juli 2023

Schaden: Die als Dateimanager getarnten Apps leiteten unbekannte Mengen an sensiblen Nutzerdaten heimlich an Server in China weiter.

MICROSOFT

Was? Ein gestohlener Schlüssel funktionierte möglicherweise nicht nur bei Exchange Online, sondern war zudem eine Art Master Key für große Teile der Microsoft Cloud.

Wie? Cyberangriff

Wann? Juli 2023

Schaden: Ob diese Möglichkeiten tatsächlich genutzt wurden, weiß man nicht, denn Microsoft versteckt sich hinter nichtssagenden Dementis.

NATO

Was? Cyberkriminelle raubten sensible Dokumente aus einem Kooperationsportal der NATO und boten diese auf Telegram zum Download an.

Wie? Cyberangriff

Wann? Juli 2023

Schaden: 845 MB geheime Kommunikationsdaten zwischen 31 Nationen wurden veröffentlicht.

QTRUST® Admin Proxy

Sicherer Zugriff. Zuverlässig!

QGROUP GMBH

WE SECURE IT.

GREAT BRITAIN

Was? Unbekannte hatten über ein Jahr lang Zugriff auf personenbezogene Daten von mehr als 40 Millionen Menschen, die sich für Wahlen in Großbritannien registriert hatten.

Wie? Cyberangriff

Wann? August 2023

Schaden: Bislang konnte kein Schaden definiert werden.

Department of Health Care Policy and Finance (HCPF)

Was? Mehr als 4 Millionen Menschen in den USA wurden über einen Leak ihrer Gesundheitsdaten informiert.

Wie? Cyberangriff

Wann? August 2023

Schaden: Die Anzahl derer, denen Daten gestohlen und missbräuchlich verwendet wurden, blieb unklar.

NISC

Was? Mutmaßlich in chinesischen Diensten stehende Hacker verschafften sich Zugriff auf die Systeme von Japans Cyberabwehrbehörde NISC.

Wie? Cyberangriff

Wann? August 2023

Schaden: Bis zu neun Monate lang hatten Hacker Zugriff auf Systeme der NISC. Der Schaden blieb unbekannt.

HACK OF THE YEAR

BITFINEX

Was? Ein New Yorker Ehepaar hat sich schuldig bekannt, fast 120.000 Bitcoin von der Kryptobörse Bitfinex gestohlen und gewaschen zu haben.

Wie? Cyberangriff

Wann? August 2023

Schaden: Wie groß der wirtschaftliche Schaden war, wurde nicht veröffentlicht. Große Teile der Beute konnten jedoch nachverfolgt und gesichert werden.

Deutsche Leasing

Was? Ein Cyberangriff auf das Leasingunternehmen führte zur Abschaltung deren Systeme.

Wie? Cyberangriff

Wann? September 2023

Schaden: Die Angreifer konnten trotz der ergriffenen Gegenmaßnahmen auf Daten und Server zugreifen. Im Nachgang tauchten Dokumenten der Deutschen Leasing im Darknet auf.

ISt GH INTERNATIONALER STRAFGERICHTSHOF

Was? Der Internationale Strafgerichtshof hat nach eigenen Angaben »anomale Aktivitäten in seinen IT-Systemen entdeckt«.
Weitere Informationen wurden nicht veröffentlicht.

Wie? Cyberangriff

Wann? September 2023

Schaden: Über einen möglichen Schaden wurde nichts bekannt.

MotelOne

Was? Die Cybercrime Gang AlphV verschaffte sich Zugriff auf das Netzwerk der Hotelkette und erbeutete über 6 Terabyte interne Daten.

Wie? Cyberangriff

Wann? September 2023

Schaden: Viele Terabytes interner Daten der Hotelkette stehen offen im Darknet. Darunter befinden sich auch Buchungs- und Zahlungsinformationen und interne Zugänge.

BaFin

Was? Die Webseite der deutschen BaFin war über mehrere Tage nicht erreichbar. Grund dafür soll eine DDoS-Attacke gewesen sein.

Wie? DDoS-Angriff

Wann? September 2023

Schaden: Die Dienste der Webseite waren nicht erreichbar. Neben dem Imageverlust entstanden der Behörde organisatorische Kosten.

AirEuropa

Was? Bei einem Cyberangriff auf die spanische Fluggesellschaft wurden Kreditkartendaten offengelegt.

Wie? Cyberangriff

Wann? Oktober 2023

Schaden: Wie viele Kunden von dem Cyberangriff betroffen waren und welche finanziellen Auswirkungen diese Attacke hatte, wurde nicht veröffentlicht.

MESSE ESSEN

Was? Die Täter drangen in den Kartenshop der Messe-Website ein und griffen dort personenbezogene Daten wie Adressen und E-Mails ab.

Wie? Ransomware

Wann? Oktober 2023

Schaden: Das Schadenausmaß blieb unbekannt.

QTRUST® SecOps

Alles im Blick:
Security Operations
und Managed Services

QGROUP GMBH

WE SECURE IT.

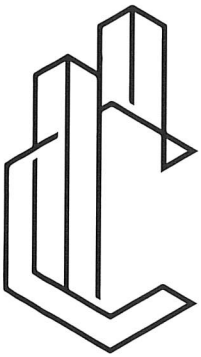
MEHRERE DEUTSCHE STÄDTE

Was? Hacker legten Webseiten mehrerer deutscher Städte lahm.

Wie? DDoS-Angriff

Wann? Oktober 2023

Schaden: Mehrere deutsche Städte, darunter Frankfurt, Köln, Dortmund und Dresden hatten mit DDoS-Angriffen zu kämpfen.
Die Erreichbarkeit der Webseiten der Kommunen war beeinträchtigt.



Südwestfalen IT

Was? Der IT-Dienstleister nahm seine Systeme infolge eines Cyberangriffs vom Netz.

Wie? Cyberangriff

Wann? Oktober 2023

Schaden: Mindestens 70 Kommunen konnten den Bürgen mehrere Tage online keine Services anbieten.

SHIMANO

Was? Cyberkriminelle raubten dem japanischen Hersteller für Fahrrad- und Angelteile Terabytes interner Daten.

Wie? Cyberangriff

Wann? November 2023

Schaden: Die Eindringlinge stahlen Daten und versuchten das Unternehmen zu erpressen. Shimano ließ das Ultimatum jedoch verstreichen und blieb standhaft.

TARGOBANK

Was? Nach Zugriffsversuchen bösartiger Akteure auf das Online-Banking hat die Bank den Zugang tausender Kunden gesperrt. Neue Zugangsdaten mussten erstellt werden.

Wie? Cyberangriff

Wann? November 2023

Schaden: Weiterer Schaden scheint nicht entstanden zu sein. Der Bank zufolge wurden die Zugriffsversuche offenbar erfolgreich abgewehrt.

TOYOTA

Was? Nach erfolgreicher Cyberattacke drohten die Angreifer, interne Daten vom Financial Service des Automobilherstellers zu leaken.

Wie? Cyberangriff

Wann? November 2023

Schaden: Die Erpresser von der Medusa-Bande forderten 8 Millionen US-Dollar Lösegeld. Es wurde nicht bekannt, ob das Unternehmen auf die Lösegeldforderung einging.

Commerzbank

Was? Kriminellen ist es gelungen, von Konten einer dreistelligen Anzahl von Commerzbank-Kunden insgesamt einen zweistelligen Millionenbetrag zu stehlen.

Wie? Cyberangriff

Wann? November 2023

Schaden: Für betroffene Kunden entstand durch den Vorfall jedoch kein Schaden, da die Buchungen »bankseitig korrigiert« wurden.

Booking.com

Was? Mit auf Datendiebstahl spezialisierter Malware griffen Cyberkriminelle zunächst Hotelmitarbeiter an und verschickten dann über Booking.com betrügerische E-Mails.

Wie? Phishing

Wann? Dezember 2023

Schaden: Aufgrund der Vielzahl der Fälle ließ sich über den wirtschaftlichen Schaden nichts Exaktes sagen.

INSOMNIAC GAMES

Was? Cyberkriminelle haben nach erfolgloser Erpressung umfangreiche Datenmengen von künftigen Spielen des PlayStation-Entwicklers veröffentlicht.

Wie? Ransomware

Wann? Dezember 2023

Schaden: Bei den Daten handelte es sich um gewaltige Projekte für die nächste Dekade, bei denen es um mehrere hundert Millionen US-Dollar geht. Der wirtschaftliche Schaden für Insomniac Games ist nicht absehbar.

TESLA

Was? Eine ehemalige Tesla-Mitarbeiterin spielte Berlins Datenschützern einen USB-Stick mit mehr als 1.000 sensiblen Dokumenten von Angestellten zu.

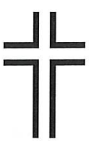
Wie? Datenverletzung

Wann? Dezember 2023

Schaden: Die Ermittlungen der Datenschutzbehörden stehen noch aus, doch der Vorfall unterstreicht die Bedeutung strenger Datenschutzmaßnahmen und das Risiko von Imageschäden für Unternehmen bei Verstößen.

ALLGAIER

Was? Der Automobilzulieferer, der sich zum Zeitpunkt des Angriffs im Insolvenzverfahren befand, wurde von Cyberkriminellen attackiert.



Wie? Cyberangriff

Wann? Dezember 2023

Schaden: Die Produktion war nicht betroffen. Über weitere Auswirkungen machten das Unternehmen und der Insolvenzverwalter keine Angaben.

Wechseln Sie Ihre **Strategie!** Bevor es zu spät ist!

Ihre Firma

Was? Unautorisierter Zugriff, Datenraub, Identitätsdiebstahl, ...

Wie? Illegale Nutzung Ihres Benutzernamens und Passwortes, Brute-Force-Attacke, Malware, ...

Wann? Heute, gestern, morgen, ...

Schaden: Imageverlust, finanzielle Einbußen, Stellenabbau, Insolvenz, ...

QGROUP GMBH

WE SECURE IT.

Haftungsansprüche gegen den Herausgeber für Schäden materieller oder ideeller Art, die durch die Nutzung oder Nichtnutzung der Informationen bzw. durch die Nutzung fehlerhafter und/oder unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, genauso wie Rechts- und Schadenersatzansprüche. Diese Broschüre inklusive aller Inhalte wurde unter größter Sorgfalt erarbeitet. Der Herausgeber übernimmt jedoch keine Gewähr für die Aktualität, Korrektheit, Vollständigkeit und Qualität der bereitgestellten Informationen. Druckfehler und Falschinformationen können nicht vollständig ausgeschlossen werden. Es kann keine juristische Verantwortung sowie Haftung in irgendeiner Form für fehlerhafte Angaben und daraus entstandene Folgen vom Herausgeber übernommen werden. Für die Inhalte von den in dieser Broschüre abgedruckten Internetseiten sind ausschließlich die Betreiber der jeweiligen Internetseiten verantwortlich. Der Herausgeber hat keinen Einfluss auf Gestaltung und Inhalte fremder Internetseiten und distanziert sich daher von allen fremden Inhalten.

©2024, 15. Ausgabe,1. Auflage.
QGroup GmbH, Wehrheim

QGroup GmbH ■ Am Joseph 15 ■ 61273 Wehrheim ■ Telefon: +49 69 175363-00
Telefax: +49 69 175363-60 ■ E-Mail: info@qgroup.de ■ www.qgroup.de